PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number:	10/679,654
Filing Date:	10/06/2003
Applicant(s):	Brian L. Pulito
Entitled:	TUNNELING NON-HTTP TRAFFIC THROUGH A REVERSE PROXY
Examiner:	John B. Walsh
Group Art Unit:	2151
Attorney Docket No.:	LOT920030023US1 (009U)

TRANSMITTAL OF APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Submitted herewith is Appellant's Appeal Brief in support of the Notice of Appeal with Pre-Appeals Conference Request filed December 19, 2006 and the Notice of Panel Decision from Appeal Review mailed January 17, 2007. As this Appeal Brief has been timely filed within the shortened statutory period of two months from the date of the filing of the Notice of Appeal, no extension of time under 37 C.F.R. § 1.136 is required. Notwithstanding, please charge any shortage in fees due under 37 C.F.R. §§ 1.17, 41.20, and in connection with the filing of this paper, including extension of time fees, to Deposit Account 12-2158, and please credit any excess fees to such deposit account.

Date: June 25, 2007

Respectfully submitted,

/Steven M. Greenberg/

Steven M. Greenberg
Registration No. 44,725
Customer Number 46321
Carey, Rodriguez, Greenberg & Paul, LLP
950 Peninsula Corporate Circle, Suite 3020
Boca Raton, FL 33487
Tel: (561) 922-3845
Facsimile: (561) 244-1062

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number:	10/679,654
Filing Date:	10/6/2003
Applicant(s):	Keith Bryan Knight
Entitled:	TUNELLING NON-HTTP STREAMS THROUGH A REVERSE PROXY
Examiner:	John B. Walsh
Group Art Unit:	2151
Attorney Docket No.:	LOT9-2003-0023 (7321-9U)

APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This Appeal Brief is submitted in support of the Notice of Appeal filed March 21, 2007, wherein Appellant appeals from the Examiner's rejection of claims 1-13.

I. REAL PARTY IN INTEREST

This application is assigned to International Business Machines Corporation by assignment recorded on October 6, 2003, at Reel 014592, Frame 0254.

II. RELATED APPEALS AND INTERFERENCES

Appellant is unaware of any related appeals and interferences.

III. STATUS OF CLAIMS

Claims 1-13 are pending in this Application and have been three-times rejected. It is from the multiple rejections of claims 1-13 that this Appeal is taken.

IV. STATUS OF AMENDMENTS

The claims have not been amended previously and their original form as of the filing date of the Application of October 6, 2003.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Independent claims 1, 6 and 9 are respectively directed to a method for tunneling non-hypertext transfer protocol (HTTP) data streams through a reverse proxy, a system for tunneling non-HTTP data streams through a reverse proxy, and a machine readable storage having stored thereon a computer program for tunneling non-HTTP data streams through a reverse proxy.

In accordance with the Appellants' invention, a socket connection can be established with a reverse proxy. Based upon the establishment of the socket connection, the socket can be passed to a non-HTTP data stream handler. The non-HTTP data stream handler can maintain the open socket connection and can write non-HTTP data streams over the socket without encapsulating the non-HTTP data within an HTTP message. The non-HTTP data stream handler can continue to exchange the non-HTTP data over the open socket until finished. Subsequently, the non-HTTP data stream handler can close the socket. Significantly, and unlike prior art HTTP tunneling implementations, in the Applicants' invention, the non-HTTP data can be exchanged over the secured connection without encapsulating the non-HTTP data within HTTP messages.

VI. ISSUES TO BE REVIEWED ON APPEAL

Claims 1 through 13 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,081,900 to Subramaniam et al. (Subramaniam).

VII. THE ARGUMENT

THE REJECTION OF CLAIMS 1-13 UNDER 35 U.S.C. § 103 AS BEING UNPATENTABLE OVER UNITED STATES PATENT NO. 6,081,900 TO SUBRAMANIAM.

For convenience of the Honorable Board in addressing the rejections, claims 2-5 stand or fall together with independent claim 1, claims 7-8 stand or fall together with claim 6, and claims 10-13 stand or fall together with independent claim 9.

I. Subramanium Does Not Teach Exchanging non-HTTP Data over a secured connection without encapsulating the non-HTTP data within HTTP Messages

Presently, claim 1 reads as follows:

> 1. A method for tunneling non-hypertext transfer protocol (HTTP) data streams through a reverse proxy, the method comprising the steps of:
>
> soliciting a secured connection with a reverse proxy protecting a back-end server computing device;
>
> establishing a connection with said back-end server computing device via said reverse proxy through said solicitation; and,
>
> responsive to establishing said connection, maintaining said connection and exchanging non-HTTP data over said secured connection without encapsulating said non-HTTP data within HTTP messages.

Similar limitations appear in the remaining independent claims 6 and 9. Notably, in the Responses filed on September 29, 2005 and on October 17, 2006, the Applicant argued that Subramanium failed to teach the exchange of non-HTTP data over a secure connection without encapsulating the

non-HTTP data within HTTP messages as expressly required by the plain claim language of claims 1, 6 and 9.

In the Final Office Action dated October 17, 2006, the Examiner relied exclusively upon Figures 1 and 2, column 7, lines 65-67 and column 11, line 30 of Subramanium in support of the argument that Srimuang teaches and suggests the exchange of non-HTTP data over a secure connection without encapsulating the non-HTTP data within HTTP messages. The Applicant, however, duly noted in both Responses that Subramanium by its own admission always requires the use of HTTP data within HTTP messages in direct contravention of Applicant's claims 1, 6 and 9. In this regard, Applicant points to column 3, lines 40 through 50 of Subramaniam, column 3 line 66 through column 4, line 19 of Subramaniam, column 7, lines 1 through 35 of Subramaniam, and column 8 lines 13 through 23 of Subramaniam, in which a "border manager" can re-write a URL of an incoming request associated with secure data from an "http" header to a "https" header in order to invoke "HTTPS" treatment.

As it is understood in the art, HTTPS is HTTP over an SSL connection. The messages exchanged in HTTPS are HTTP messages. The HTTP messages, however, are exchanged using SSL connectivity. Column 7, lines 24 through 35 of Subramaniam discuss the nature of HTTPS and reference United States Patent No. 5,825,890 to Elgamal et al. (Elgamal). With specific reference to Elgamal, it is stated with particularity:

> [T]he HTTPS header in the URL indicates that the server is a secure HTTP server. The "S" suffix in the header syntax indicates that the connection is to be a secure connection, and that the application should invoke the SSL library. The absence of an "S" from the header syntax, that is a normal HTTP header, would indicate that the connection need not be secure, and that the SSL library need not be invoked. Thus, the HTTPS header indicates to the application that the SSL library is to be called to provide a secure HTTP transfer. **Note that the protocol known as HTTP itself is not altered or modified.** Rather, information transferred between client and server applications is encrypted/decrypted in transit using the client side and server side SSL libraries. In effect, the SSL libraries provide an additional security layer between application and transport layers. See Elgamal column 14, line 55 through column 15. line 3 (emphasis added).

The emphasized portion of the Elgamal citation can be found on column 14, lines 64 through 65.

Considering the teachings of Subramaniam and Elgamal, in the claims of the Applicants' Patent Application, it is explicitly required that "non-HTTP data" is written to a reverse proxy "without encapsulating said non-HTTP data within HTTP messages". Clearly, the "without encapsulating said non-HTTP data within HTTP messages" is not shown by Subramaniam because Subramaniam requires the use of HTTP messages inherent to HTTP. Thus, the Applicants respectfully believe that Subramaniam cannot be held to teach each and every recited limitation of claims 1, 6 and 9.

II. The Examiner Cannot Cite Subramanium in Support of a Rejection under 35 U.S.C. § 103(a) based upon what is not taught in Subramanium.

M.P.E.P. § 2143 expressly requires that to establish a prima facie, all elements of a claim must be present or suggested by the cited art. The Examiner, in this case, has relied upon a reference not for what the reference teaches, but for what the reference does not teach. Specifically, the Examiner referenced column 7, lines 65-67 of Subramaniam in which it states, "FTP files, gopher resources, and other data on the target server 104 may be handled in a similar manner." The Examiner without further analysis justified an obviousness based rejection on this single phrase by stating, "Subramaniam et al. discloses one of ordinary skill in the art could use other protocols, such as FTP, for exchanging data."

By the Examiner's logic Subramanium teaches that FTP can be used as a protocol and, because Subramanium says nothing further, it must be that Subramanium teaches the exchange of FTP data over a secured connection without encapsulating FTP data in an HTTP message. Of course, Subramanium provides no teaching of any exchange of FTP data outside of the HTTP protocol and in fact it is well known and accepted that one can access an FTP server through a Web

browser to retrieve a file in which the FTP data representative of the file is encapsulated within HTTP messages. The Examiner has failed, however, to recite a single portion of Subramanium disclosing the exchange of FTP data outside of HTTP. To wit, simply because Subramanium does not affirmatively teach the exchange of FTP data through HTTP messages (because Subramanium says nothing other the mentioning "FTP files"), does not mean that Subramanium implicitly teaches the exchange of FTP data outside of HTTP. Yet, as repeatedly noted by the Applicant in the Responses of September 29, 2005 and on October 17, 2006, the plain text of Subramanium in column 7 requires the use of HTTP messages for all exchanges of data in the secure connection.

III. Conclusion

Based upon the foregoing, Appellant respectfully submit that the Examiner's rejections under 35 U.S.C. § 103(a) for obviousness based upon the applied prior art are not viable. Appellants, therefore, respectfully solicit the Honorable Board to reverse the Examiner's rejections under 35 U.S.C. § 103(a).

Date: June 25, 2007

Respectfully submitted,

/Steven M. Greenberg/
Steven M. Greenberg
Registration No. 44,725
Customer Number 46321
Carey, Rodriguez, Greenberg & Paul, LLP
950 Peninsula Corporate Circle, Suite 3020
Boca Raton, FL 33487
Tel: (561) 922-3845
Facsimile: (561) 244-1062

VIII. CLAIMS APPENDIX

1. (Original) A method for tunneling non-hypertext transfer protocol (HTTP) data streams through a reverse proxy, the method comprising the steps of:

soliciting a secured connection with a reverse proxy protecting a back-end server computing device;

establishing a connection with said back-end server computing device via said reverse proxy through said solicitation; and,

responsive to establishing said connection, maintaining said connection and exchanging non-HTTP data over said secured connection without encapsulating said non-HTTP data within HTTP messages.

2. (Original) The method of claim 1, wherein said soliciting step comprises the step of requesting a secured sockets layer (SSL) connection with said reverse proxy.

3. (Original) The method of claim 2, wherein said requesting step comprises the steps of:

acquiring an address for said reverse proxy and a port for establishing an SSL connection with said reverse proxy;

further acquiring an address for said back-end server computing device and a port for establishing an SSL connection with said back-end server computing device;

formulating an HTTP-CONNECT message using said acquired addresses and ports; and,

writing said formulated HTTP-CONNECT message to said reverse proxy.

4. (Original) The method of claim 1, wherein said exchanging step comprises the steps of:

formatting a buffer with real-time data; and,

writing said buffer to said secured connection.

5. (Original) The method of claim 1, further comprising the step of performing authentication in said reverse proxy as a condition of establishing said secured connection.

6. (Original) A system for tunneling non-hypertext transfer protocol (HTTP) data streams through a reverse proxy, the system comprising:

a reverse proxy disposed between a client computing device and a server computing device in a computer communications network;

an authentication process configured for operation in conjunction with said reverse proxy;

a communications socket established between said reverse proxy and said client computing device; and,

a non-HTTP data handler coupled to said secured communications socket and programmed to write non-HTTP data to said reverse proxy without encapsulating said non-HTTP data within HTTP messages.

7. (Original) The system of claim 6, wherein server computing device is a real-time streaming media server, said non-HTTP data handler is a real-time streaming media client, and said non-HTTP data is real-time streaming media.

8. (Original) The system of claim 6, wherein said communications socket is a secured sockets layer (SSL) communications link.

9. (Original) A machine readable storage having stored thereon a computer program for tunneling non-hypertext transfer protocol (HTTP) data streams through a reverse proxy, the computer program comprising a routine set of instructions for causing the machine to perform the steps of:

soliciting a secured connection with a reverse proxy protecting a back-end server computing device;

establishing a connection with said back-end server computing device via said reverse proxy through said solicitation; and,

responsive to establishing said connection, maintaining said connection and exchanging non-HTTP data over said secured connection without encapsulating said non-HTTP data within HTTP messages.

10. (Original) The machine readable storage of claim 9, wherein said soliciting step comprises the step of requesting a secured sockets layer (SSL) connection with said reverse proxy.

11. (Original) The machine readable storage of claim 10, wherein said requesting step comprises the steps of:

acquiring an address for said reverse proxy and a port for establishing an SSL connection with said reverse proxy;

further acquiring an address for said back-end server computing device and a port for establishing an SSL connection with said back-end server computing device;

formulating an HTTP-CONNECT message using said acquired address and port; and,

writing said formulated HTTP-CONNECT message to said reverse proxy.

12. (Original) The machine readable storage of claim 9, wherein said exchanging step comprises the steps of:

formatting a buffer with real-time data; and,

writing said buffer to said secured connection.

13. (Original) The machine readable storage of claim 9, further comprising the step of performing authentication in said reverse proxy as a condition of establishing said secured connection.

IX. EVIDENCE APPENDIX

No evidence submitted pursuant to 37 C.F.R. §§ 1.130, 1.131, or 1.132 of this title or of any other evidence entered by the Examiner has been relied upon by Appellant in this Appeal, and thus no evidence is attached hereto.

X. RELATED PROCEEDINGS APPENDIX

Since Appellant is unaware of any related appeals and interferences, no decision rendered by a court or the Board is attached hereto.